Monetary Authority of Singapore

TECHNOLOGY RISK MANAGEMENT GUIDELINES

JUNE 2013

TABLE OF CONTENTS

1 INTRODUCTION

1.0.1 The advancement of information technology ("IT") has brought about rapid changes to the way businesses and operations are being conducted in the financial industry. IT is no longer a support function within a financial institution[1] ("FI") but a key enabler for business strategies including reaching out to and meeting customer needs.

1.0.2 Financial systems and networks supporting FIs' business operations have also grown in scope and complexity over the years. FIs offering a diversity of products and services could have their financial systems operating in multiple locations and supported by different service providers.

1.0.3 FIs are also faced with the challenge of keeping pace with the needs and preferences of consumers who are getting more IT-savvy and switching to internet and mobile devices for financial services, given their speed, convenience and ease of use. Increasingly, FIs are deploying more advanced technology and online systems, including internet banking systems, mobile banking and payment systems, online trading platforms and insurance portals, to reach their customers. In this regard, FIs should fully understand the magnitude and intensification of technology risks from these systems. They should also put in place adequate and robust risk management systems as well as operating processes to manage these risks.

1.0.4 The Technology Risk Management Guidelines (the "Guidelines") set out risk management principles and best practice standards to guide the FIs in the following:

a. Establishing a sound and robust technology risk management framework;

b. Strengthening system security, reliability, resiliency, and recoverability; and

c. Deploying strong authentication to protect customer data, transactions and systems.

1.0.5 While the Guidelines are not legally binding, the degree of observance with the spirit of the Guidelines by an FI is an area of consideration in the risk assessment of the FI by MAS.

[1] Financial institution has the same meaning as in section 27A(6) of the Monetary Authority of Singapore Act (Cap. 186).

2 APPLICABILITY OF THE GUIDELINES

2.0.1 The Guidelines are statements of industry best practices which FIs are expected to adopt. The Guidelines do not affect, and should not be regarded as a statement of the standard of care owed by FIs to their customers. Where appropriate, FIs may adapt these guidelines, taking into account the diverse activities they engage in and the markets in which they conduct transactions. FIs should read the Guidelines in conjunction with relevant regulatory requirements and industry standards.

2.0.2 The objective of the Guidelines is to promote the adoption of sound practices and processes for managing technology.

3 OVERSIGHT OF TECHNOLOGY RISKS BY BOARD OF DIRECTORS AND SENIOR MANAGEMENT

3.0.1 IT is a core function of many FIs. When critical systems fail and customers cannot access their accounts, an FI's business operations may immediately come to a standstill. The impact on customers would be instantaneous, with significant consequences to the FI, including reputational damage, regulatory breaches, revenue and business losses.

3.0.2 In view of the importance of the IT function in supporting an FI's business, the board of directors and senior management should have oversight of technology risks and ensure that the organisation's IT function is capable of supporting its business strategies and objectives.

3.1 Roles and Responsibilities

3.1.1 The board of directors and senior management should ensure that a sound and robust technology risk management framework is established and maintained. They should also be involved in key IT decisions.

3.1.2 They should also be fully responsible for ensuring that effective internal controls and risk management practices are implemented to achieve security, reliability, resiliency and recoverability.

3.1.3 The board of directors and senior management should give due consideration to cost-benefit issues, including factors such as reputation, customer confidence, consequential impact and legal implications, with regard to investment in controls and security measures for computer systems, networks, data centres ("DC"), operations and backup facilities.

3.2 IT Policies, Standards and Procedures

3.2.1 FIs should establish IT policies, standards and procedures, which are critical components of the framework, to manage technology risks and safeguard information system assets[2] in the organisation.

3.2.2 Due to rapid changes in the IT operating and security environment, policies, standards and procedures should be regularly reviewed and updated.

[2] Information systems assets refer to data, systems, network devices and other IT equipment.

3.2.3 Compliance processes should be implemented to verify that IT security standards and procedures are enforced. Follow-up processes should be implemented so that compliance deviations are addressed and remedied on a timely basis.

3.3 People Selection Process

3.3.1 Careful selection of staff, vendors and contractors is crucial to minimise technology risks due to system failure, internal sabotage or fraud. As people play an important role in managing systems and processes in an IT environment, the FI should implement a screening process that is comprehensive and effective.

3.3.2 Staff, vendors and contractors, who are authorised to access the FI's systems, should be required to protect sensitive or confidential information.

3.4 IT Security Awareness

3.4.1 A comprehensive IT security awareness training program should be established to enhance the overall IT security awareness level in the organisation. The training program should include information on IT security policies and standards as well as individual responsibility in respect of IT security and measures that should be taken to safeguard information system assets. Every staff in the organisation should be made aware of the applicable laws, regulations, and guidelines pertaining to the usage, deployment and access to IT resources.

3.4.2 The training program should be conducted and updated at least annually and extended to all new and existing staff, contractors and vendors who have access to the FI's IT resources and systems.

3.4.3 The training program should be endorsed by senior management. It should be reviewed and updated to ensure that the contents of the program remain current and relevant. The review should also take into consideration the evolving nature of technology as well as emerging risks.

4 TECHNOLOGY RISK MANAGEMENT FRAMEWORK

4.0.1 A technology risk management framework should be established to manage technology risks in a systematic and consistent manner. The framework should encompass the following attributes:

a. Roles and responsibilities in managing technology risks;

b. Identification and prioritisation of information system assets;

c. Identification and assessment of impact and likelihood of current and emerging threats, risks and vulnerabilities;

d. Implementation of appropriate practices and controls to mitigate risks; and

e. Periodic update and monitoring of risk assessment to include changes in systems, environmental or operating conditions that would affect risk analysis.

4.0.2 Effective risk management practices and internal controls should be instituted to achieve data confidentiality[3], system security, reliability, resiliency and recoverability in the organisation.

4.1 Information System Assets

4.1.1 Information system assets should be adequately protected from unauthorised access, misuse or fraudulent modification, insertion, deletion, substitution, suppression or disclosure.

4.1.2 The FI should establish a clear policy on information system asset protection. Criticality of information system assets should be identified and ascertained in order to develop appropriate plans to protect them.

4.2 Risk Identification

4.2.1 Risk identification entails the determination of the threats and vulnerabilities to the FI's IT environment which comprises the internal and external networks, hardware, software, applications, systems interfaces, operations and human elements.

[3] Data confidentiality refers to the protection of sensitive or confidential information such as customer data from unauthorised access, disclosure, etc.

4.2.2 A threat may take the form of any condition, circumstance, incident or person with the potential to cause harm by exploiting vulnerability in a system. The source of the threat can be natural, human or environmental. Humans are significant sources of threats through deliberate acts or omissions which could inflict extensive harm to the organisation and its information systems.

4.2.3 Security threats such as those manifested in denial of service attacks, internal sabotage and malware infestation could cause severe harm and disruption to the operations of an FI with consequential losses for all parties affected. The FI should be vigilant in monitoring such mutating and growing risks as it is a crucial step in the risk containment exercise.

4.3 Risk Assessment

4.3.1 Following risk identification, the FI should perform an analysis and quantification of the potential impact and consequences of these risks on the overall business and operations.

4.3.2 The extent of risk impact depends on the likelihood of various threat and vulnerability pairings or linkages capable of causing harm to the organisation should an adverse event occur.

4.3.3 The FI should develop a threat and vulnerability matrix to assess the impact of the threat to its IT environment. The matrix will also assist the FI in prioritising IT risks.

4.4 Risk Treatment

4.4.1 For each type of risk identified, the FI should develop and implement risk mitigation and control strategies that are consistent with the value of the information system assets and the level of risk tolerance.

4.4.2 Risk mitigation entails a methodical approach for evaluating, prioritising and implementing appropriate risk-reduction controls. A combination of technical, procedural, operational and functional controls would provide a rigorous mode of reducing risks.

4.4.3 As it may not be practical to address all known risks simultaneously or in the same timeframe, the FI should give priority to threat and vulnerability pairings with high risk ranking which could cause significant harm or impact to the FI's operations. The FI should assess its risk tolerance for damages and losses in

the event that a given risk-related event materialises. The costs of risk controls should be balanced against the benefits to be derived.

4.4.4 It is imperative that the FI is able to manage and control risks in a manner that will maintain its financial and operational viability and stability. When deciding on the adoption of alternative controls and security measures, the FI should also be conscious of costs and effectiveness of the controls with regard to the risks being mitigated.

4.4.5 The FI should refrain from implementing and running a system where the threats to the safety and soundness of the IT system are insurmountable and the risks cannot be adequately controlled.

4.4.6 As a risk mitigating measure, the FI could consider taking insurance cover for various insurable risks, including recovery and restitution costs.

4.5 Risk Monitoring and Reporting

4.5.1 The FI should maintain a risk register which facilitates the monitoring and reporting of risks. Risks of the highest severity should be accorded top priority and monitored closely with regular reporting on the actions that have been taken to mitigate them. The FI should update the risk register periodically, and institute a monitoring and review process for continuous assessment and treatment of risks.

4.5.2 To facilitate risk reporting to management, the FI should develop IT risk metrics to highlight systems, processes or infrastructure that have the highest risk exposure. An overall technology risk profile of the organisation should also be provided to the board of directors and senior management. In determining the IT risk metrics, the FI should consider risk events, regulatory requirements and audit observations.

4.5.3 Risk parameters may shift as the IT environment and delivery channels change. Thus, the FI should review and update the risk processes accordingly, and conduct a re-evaluation of past risk-control methods with renewed testing and assessment of the adequacy and effectiveness of risk management processes.

4.5.4 Management of the IT function should review and update its IT risk control and mitigation approach, taking into account changing circumstances and variations in the FI's risk profile.

5 MANAGEMENT OF IT OUTSOURCING RISKS

5.0.1 IT outsourcing comes in many forms and permutations. Some of the most common types of IT outsourcing are in systems development and maintenance, support to DC operations, network administration, disaster recovery services, application hosting, and cloud computing. Outsourcing can involve the provision of IT capabilities and facilities by a single third party or multiple vendors located in Singapore or abroad.

5.1 Due Diligence

5.1.1 The board of directors and senior management should fully understand risks associated with IT outsourcing. Before a service provider is appointed, due diligence should be carried out to determine its viability, capability, reliability, track record and financial position.

5.1.2 The FI should ensure that contractual terms and conditions governing the roles, relationships, obligations and responsibilities of all contracting parties are set out fully in written agreements. The requirements and conditions covered in the agreements would usually include performance targets, service levels, availability, reliability, scalability, compliance, audit, security, contingency planning, disaster recovery capability and backup processing facility.

5.1.3 The FI should ensure that the service provider grants access to all parties nominated by the FI to its systems, operations, documentation and facilities in order to carry out any review or assessment for regulatory, audit or compliance purposes. In addition, the engagement of the service provider should not hinder the ability of the regulatory authorities to assess the FI's IT risks which would include inspecting, supervising or examining the service provider's roles, responsibilities, obligations, functions, systems and facilities. In this regard, the FI should ensure that the contractual agreements with the service provider recognise the authority of regulators to perform an assessment on the service provider.

5.1.4 IT outsourcing should not result in any weakening or degradation of the FI's internal controls. The FI should require the service provider to employ a high standard of care and diligence in its security policies, procedures and controls to protect the confidentiality and security of its sensitive or confidential information, such as customer data, computer files, records, object programs and source codes.

5.1.5 The FI should require the service provider to implement security policies, procedures and controls that are at least as stringent as it would expect for its own operations.

5.1.6 The FI should monitor and review the security policies, procedures and controls of the service provider on a regular basis, including commissioning or obtaining periodic expert reports on security adequacy and compliance in respect of the operations and services provided by the service provider.

5.1.7 The FI should require the service provider to develop and establish a disaster recovery contingency framework which defines its roles and responsibilities for documenting, maintaining and testing its contingency plans and recovery procedures.

5.1.8 All parties concerned, including those from the service provider, should receive regular training in activating the contingency plan and executing recovery procedures.

5.1.9 The disaster recovery plan should be reviewed, updated and tested regularly in accordance with changing technology conditions and operational requirements.

5.1.10 The FI should also put in place a contingency plan based on credible worst-case scenarios for service disruptions to prepare for the possibility that its current service provider may not be able to continue operations or render the services required. The plan should incorporate identification of viable alternatives for resuming its IT operations elsewhere.

5.2 Cloud Computing

5.2.1 Cloud computing is a service and delivery model for enabling on-demand network access to a shared pool of configurable computing resources (servers, storage and services). Users of such services may not know the exact locations of servers, applications and data within the service provider's computing infrastructure for the hosting, storing or processing of information.

5.2.2 In performing its due diligence for all forms of outsourcing arrangements, the FI should be aware of cloud computing's unique attributes and risks especially in areas of data integrity, sovereignty, commingling, platform multi-tenancy, recoverability and confidentiality, regulatory compliance, auditing and data offshoring.

5.2.3 As cloud computing service providers may adopt multi-tenancy and data commingling architectures in order to process data for multiple customers, the FI should pay attention to these service providers' abilities to isolate and clearly identify its customer data and other information system assets for protection.

5.2.4 In the event of contract termination with the service provider, either on expiry or prematurely, the FI should have the contractual power and means to promptly remove or destroy data stored at the service provider's systems and backups.

5.2.5 The FI should verify the service provider's ability to recover the outsourced systems and IT services within the stipulated recovery time objective ("RTO") prior to contracting with the service provider.

6 ACQUISITION AND DEVELOPMENT OF INFORMATION SYSTEMS

6.0.1 Many systems fail because of poor system design and implementation, as well as inadequate testing. The FI should identify system deficiencies and defects at the system design, development and testing phases.

6.0.2 The FI should establish a steering committee, consisting of business owners, the development team and other stakeholders to provide oversight and monitoring of the progress of the project, including deliverables to be realised at each phase of the project and milestones to be reached according to the project timetable.

6.1 IT Project Management

6.1.1 In drawing up a project management framework, the FI should ensure that tasks and processes for developing or acquiring new systems include project risk assessment and classification, critical success factors for each project phase, definition of project milestones and deliverables. The FI should clearly define in the project management framework, the roles and responsibilities of staff involved in the project.

6.1.2 The FI should clearly document project plans for all IT projects. In the project plans, the FI should set out clearly the deliverables to be realised at each phase of the project as well as milestones to be reached.

6.1.3 The FI should ensure that user functional requirements, business cases, cost-benefit analysis, systems design, technical specifications, test plans and service performance expectation are approved by the relevant business and IT management.

6.1.4 The FI should establish management oversight of the project to ensure that milestones are reached and deliverables are realised in a timely manner. The FI should escalate issues or problems which could not be resolved at the project committee level to senior management for attention and intervention.

6.2 Security Requirements and Testing

6.2.1 The FI should clearly specify security requirements relating to system access control, authentication, transaction authorisation, data integrity, system activity logging, audit trail, security event tracking and exception handling in the early

phase of system development or acquisition. The FI should also perform a compliance check on the FI's security standards against the relevant statutory requirements.

6.2.2 A methodology for system testing[4] should be established. The scope of tests should cover business logic, security controls and system performance under various stress-load scenarios and recovery conditions.

6.2.3 The FI should ensure that full regression testing is performed before system rectification or enhancement is implemented. Users whose systems and operations are affected by the system changes should review and sign off on the outcome of the tests (Refer to Appendix A for details on Systems Security Testing and Source Code Review).

6.2.4 The FI should conduct penetration testing prior to the commissioning of a new system which offers internet accessibility and open network interfaces. The FI should also perform vulnerability scanning of external and internal network components that support the new system.

6.2.5 The FI should maintain separate physical or logical environments for unit, integration, as well as system and user acceptance testing ("UAT"), and closely monitor vendor and developers' access to UAT environment.

6.3 Source Code Review

6.3.1 There are different ways of coding programs which may conceal security threats and loopholes, deliberate or unintentional. System and user acceptance tests are usually ineffective in detecting malicious codes, trojans, backdoors, logic bombs and other malware. Black-box testing is not an effective tool in identifying or detecting these security threats and weaknesses.

6.3.2 Source code review is a methodical examination of the source code of an application with the objective of finding defects that are due to coding errors, poor coding practices or malicious attempts. It is designed to identify security vulnerabilities and deficiencies, and mistakes in system design or functionality relating to areas such as control structure, security, input validation, error handling, file update, function parameter verification, before the system is implemented.

[4] System testing is broadly defined to include unit, modular, integration, system and user acceptance testing.

6.3.3 The FI should ensure that there is a high degree of system and data integrity for all systems. The FI should exercise due diligence in ensuring its applications have appropriate security controls, taking into consideration the type and complexity of services these applications provide.

6.3.4 Based on the FI's risk analysis, the FI should rigorously test specific application modules and security safeguards with a combination of source code review, exception testing and compliance review to identify errant coding practices and systems vulnerabilities that could lead to security problems, violations and incidents.

6.4 End User Development

6.4.1 There are common business application tools and software which allow business users to develop simple applications to automate their operations, perform data analysis and generate reports for the FI and customers.

6.4.2 The FI should perform an assessment to ascertain the importance of these applications to the business.

6.4.3 Recovery measures, user access and data protection controls, at the minimum, should be implemented for such applications.

6.4.4 The FI should review and test end user developed program codes, scripts and macros before they are used so as to ensure the integrity and reliability of the applications.

7 IT SERVICE MANAGEMENT

7.0.1 A robust IT service management framework is essential for supporting IT systems, services and operations, managing changes, incidents and problems as well as ensuring the stability of the production IT environment.

7.0.2 The framework should comprise the governance structure, processes and procedures for change management, software release management, incident and problem management as well as capacity management.

7.1 Change Management

7.1.1 The FI should establish a change management process to ensure that changes to production systems are assessed, approved, implemented and reviewed in a controlled manner.

7.1.2 The change management process should apply to changes pertaining to system and security configurations, patches for hardware devices and software updates.

7.1.3 Prior to deploying changes to the production environment, the FI should perform a risk and impact analysis of the change request in relation to existing infrastructure, network, up-stream and downstream systems. The FI should also determine if the introduced change would spawn security implications or software compatibility problems to affected systems or applications.

7.1.4 The FI should adequately test the impending change and ensure that it is accepted by users prior to the migration of the changed modules to the production system. The FI should develop and document appropriate test plans for the impending change. The FI should obtain test results with user sign-offs prior to the migration.

7.1.5 All changes to the production environment should be approved by personnel delegated with the authority to approve change requests.

7.1.6 To minimise risks associated with changes, FIs should perform backups of affected systems or applications prior to the change. The FI should establish a rollback plan to revert to a former version of the system or application if a problem is encountered during or after the deployment. The FI should establish alternative recovery options to address situations where a change does not allow the FI to revert to a prior status.

7.1.7 Audit and security logs are useful information which facilitates investigations and trouble shooting. The FI should ensure that the logging facility is enabled to record activities that are performed during the migration process.

7.2 Program Migration

7.2.1 Program migration involves the movement of software codes and scripts from the development environment to test and production environments. Unauthorised and malicious codes which are injected during the migration process could compromise data, systems and processes in the production environment.

7.2.2 Separate physical or logical environments for systems development, testing, staging and production should be established.

7.2.3 Where controls in the non-production environment are different or less stringent from those in the production environment, the FI should perform a risk assessment and ensure that sufficient preventive and detective controls have been implemented before connecting a non-production environment to the internet.

7.2.4 Segregation of duties should be enforced so that no single individual has the ability to develop, compile and move object codes from one environment to another.

7.2.5 After a change has been successfully implemented in the production environment, the change should also be replicated and migrated to disaster recovery systems or applications for consistency.

7.3 Incident Management

7.3.1 An IT incident occurs when there is an unexpected disruption to the standard delivery of IT services. The FI should appropriately manage such incidents to avoid a situation of mishandling that result in a prolonged disruption of IT services or further aggravation.

7.3.2 The FI should establish an incident management framework with the objective of restoring normal IT service as quickly as possible following the incident, and with minimal impact to the FI's business operations. The FI should also establish the roles and responsibilities of staff involved in the incident

management process, which includes recording, analysing, remediating and monitoring incidents.

7.3.3 It is important that incidents are accorded with the appropriate severity level. As part of incident analysis, the FI may delegate the function of determining and assigning incident severity levels to a centralised technical helpdesk function. The FI should train helpdesk staff to discern incidents of high severity level. In addition, criteria used for assessing severity levels of incidents should be established and documented.

7.3.4 The FI should establish corresponding escalation and resolution procedures where the resolution timeframe is commensurate with the severity level of the incident.

7.3.5 The predetermined escalation and response plan for security incidents[5], should be tested on a regular basis.

7.3.6 The FI should form a computer emergency response team, comprising staff within the FI with necessary technical and operational skills to handle major incidents.

7.3.7 In some situations, major incidents may further develop unfavourably into a crisis. Senior management should be kept apprised of the development of these incidents so that the decision to activate the disaster recovery plan can be made on a timely basis. FIs should inform MAS as soon as possible in the event that a critical system has failed over to its disaster recovery system. Procedures to notify MAS of these incidents should be established.

7.3.8 Being able to maintain customer confidence throughout a crisis or an emergency situation is of great importance to the reputation and soundness of the FI. FIs should include in their incident response procedures a predetermined action plan to address public relations issues.

7.3.9 The FI should keep customers informed of any major incident. The FI should also assess the effectiveness of the mode of communication, including informing the general public, where necessary.

7.3.10 As incidents may stem from numerous factors, FIs should perform a root-cause and impact analysis for major incidents which result in severe disruption

[5] Examples of security incidents include virus outbreak, malware infiltration, systems hacking, account impersonation or compromise, phishing attack, internal sabotage or denial of service attacks.

of IT services. The FI should take remediation actions to prevent the recurrence of similar incidents.

7.3.11 The FI should include in its incident report an executive summary of the incident, an analysis of root cause which triggered the event, its impact as well as measures taken to address the root cause and consequences of the event.

7.3.12 The root-cause and impact analysis report should cover the following areas:

a. Root Cause Analysis

i. When did it happen?

ii. Where did it happen?

iii. Why and how did the incident happen?

iv. How often had a similar incident occurred over the last 3 years?

v. What lessons were learnt from this incident?

b. Impact Analysis

i. Extent, duration or scope of the incident including information on the systems, resources, customers that were affected;

ii. Magnitude of the incident including foregone revenue, losses, costs, investments, number of customers affected, implications, consequences to reputation and confidence; and

iii. Breach of regulatory requirements and conditions as a result of the incident.

c. Corrective and Preventive Measures

i. Immediate corrective action to be taken to address consequences of the incident. Priority should be placed on addressing customers' concerns and / or compensation;

ii. Measures to address the root cause of the incident; and

iii. Measures to prevent similar or related incidents from occurring.

7.3.13 The FI should adequately address all incidents within corresponding resolution timeframes and monitor all incidents to their resolution.

7.4 Problem Management

7.4.1 While the objective of incident management is to restore the IT service as soon as possible, the aim of problem management is to determine and eliminate the root cause to prevent the occurrence of repeated problems.

7.4.2 The FI should establish clear roles and responsibilities of staff involved in the problem management process. The FI should identify, classify, prioritise and address all problems in a timely manner.

7.4.3 To facilitate the classification process, the FI should clearly define criteria to categorise problems by severity level. To effectively monitor and escalate problems, the FI should establish target resolution time as well as appropriate escalation processes for each severity level.

7.4.4 A trend analysis of past incidents should be performed to facilitate the identification and prevention of similar problems.

7.5 Capacity Management

7.5.1 To ensure that IT systems and infrastructure are able to support business functions, the FI should ensure that indicators such as performance, capacity and utilisation are monitored and reviewed.

7.5.2 The FI should establish monitoring processes and implement appropriate thresholds to provide sufficient time for the FI to plan and determine additional resources to meet operational and business requirements effectively.

8 SYSTEMS RELIABILITY, AVAILABILITY AND RECOVERABILITY

8.0.1 The reliability, availability, and recoverability of IT systems, networks and infrastructures are crucial in maintaining confidence and trust in the operational and functional capabilities of an FI. When critical systems fail, the disruptive impact on the FI's operations or customers will usually be severe and widespread and the FI may suffer serious consequences to its reputation.

8.0.2 As all systems are vulnerable, the FI should define its recovery and business resumption priorities. The FI should also test and practise its contingency procedures so that disruptions to its business arising from a serious incident may be minimised.

8.1 Systems Availability

8.1.1 Important factors associated with maintaining high system availability are adequate capacity, reliable performance, fast response time, scalability and swift recovery capability.

8.1.2 An FI may employ a number of complex interdependent systems and network components for its IT processing. An entire system can become inoperable when a single critical hardware component or software module malfunctions or is damaged. The FI should develop built-in redundancies to reduce single points of failure which can bring down the entire network. The FI should maintain standby hardware, software and network components that are necessary for fast recovery.

8.1.3 The FI should achieve high availability[6] for critical systems[7].

8.2 Disaster Recovery Plan

8.2.1 In formulating and constructing a rapid recovery plan, the FI should include a scenario analysis to identify and address various types of contingency scenarios. The FI should consider scenarios such as major system outages

[6] Other than during periods of planned maintenance, the FI should enhance its system and infrastructure resiliency by deploying suitable solutions, e.g., active-active setup, for these systems to minimise downtime.

[7] Critical system means a system, the failure which will cause significant disruption to the operations of the FI or materially impact the FI's service to its customers. "System" means any hardware, software, network or IT component which is part of an IT infrastructure.

which may be caused by system faults, hardware malfunction, operating errors or security incidents, as well as a total incapacitation of the primary DC.

8.2.2 IT incidents, if handled inappropriately, may escalate into situations that have a severe impact on the FI's operations or its customers. The FI should evaluate the recovery plan and incident response procedures at least annually and update them as and when changes to business operations, systems and networks occur.

8.2.3 To strengthen recovery measures relating to large scale disruptions and to achieve risk diversification, the FI should implement rapid backup and recovery capabilities at the individual system or application cluster level. The FI should consider inter-dependencies between critical systems in drawing up its recovery plan and conducting contingency tests.

8.2.4 The FI should define system recovery and business resumption priorities and establish specific recovery objectives including RTO and recovery point objective (RPO) for IT systems and applications. RTO is the duration of time, from the point of disruption, within which a system should be restored. RPO refers to the acceptable amount of data loss for an IT system should a disaster occur.

8.2.5 The FI should establish a recovery site that is geographically separate from the primary site to enable the restoration of critical systems and resumption of business operations should a disruption occur at the primary site.

8.2.6 The required speed of recovery will depend on the criticality of resuming business operations, the type of services and whether there are alternative ways and processing means to maintain adequate continuing service levels to satisfy customers. The FI may wish to explore recovery strategies and technologies such as on-site redundancy and real-time data replication to enhance the FI's recovery capability.

8.2.7 The resiliency and robustness of critical systems which are outsourced to offshore service providers is highly dependent on the stability and availability of cross-border network links. To minimise impact on business operations in the event of a disruption (e.g. due to earthquake), the FI should ensure that cross-border network redundancy, with strategies such as engagement of different network service providers and alternate network paths, is instituted.

8.3 Disaster Recovery Testing

8.3.1 During a system outage, the FI should refrain from adopting impromptu and untested recovery measures over pre-determined recovery actions that have been rehearsed and approved by management. Ad hoc recovery measures carry high operational risks as their effectiveness has not been verified through rigorous testing and validation.

8.3.2 The FI should test and validate at least annually the effectiveness of recovery requirements and the ability of staff to execute the necessary emergency and recovery procedures.

8.3.3 Various scenarios, including total shutdown or incapacitation of the primary site as well as component failure at the individual system or application cluster level, should be covered in disaster recovery tests.

8.3.4 The FI should test the recovery dependencies between systems. Bilateral or multilateral recovery testing should be conducted where networks and systems are linked to specific service providers and vendors.

8.3.5 The FI should involve its business users in the design and execution of comprehensive test cases to verify that recovered systems function properly. The FI should also participate in disaster recovery tests that are conducted by its service provider(s), including those systems which are located offshore.

8.4 Data Backup Management

8.4.1 The FI should develop a data backup strategy for the storage of critical information.

8.4.2 As part of the data backup and recovery strategy, FIs may implement specific data storage architectures such as Direct-Attached Storage (DAS), Network-Attached Storage (NAS) or Storage Area Network (SAN) sub-systems connected to production servers. In this regard, processes should be in place to review the architecture and connectivity of sub disk storage systems for single points of failure and fragility in functional design and specifications, as well as the technical support by service providers (Refer to Appendix B for details on Storage System Resiliency).

8.4.3 The FI should carry out periodic testing and validation of the recovery capability of backup media and assess if the backup media is adequate and sufficiently effective to support the FI's recovery process.

8.4.4 The FI should encrypt backup tapes and disks, including USB disks, containing sensitive or confidential information before they are transported offsite for storage.

9 OPERATIONAL INFRASTRUCTURE SECURITY MANAGEMENT

9.0.1 The IT landscape is vulnerable to various forms of cyber attacks[8], and the frequency and malignancy of attacks are increasing. It is imperative that FIs implement security solutions at the data, application, database, operating systems and network layers to adequately address and contain these threats.

9.0.2 Appropriate measures should be implemented to protect sensitive or confidential information such as customer personal, account and transaction data which are stored and processed in systems. Customers should be properly authenticated before access to online transaction functions and, sensitive personal or account information is permitted. Sensitive customer information including login credentials, passwords and personal identification numbers (PINs) should be secured against exploits such as ATM skimming, card cloning, hacking, phishing and malware.

9.1 Data Loss Prevention

9.1.1 Internal sabotage, clandestine espionage or furtive attacks by trusted staff, contractors and vendors are potentially among the most serious risks that FIs could face in an increasingly complex and dynamic IT environment. Current and past staff, contractors, vendors and those who have knowledge of the inner workings of the FI's systems, operations and internal controls have a significant advantage over external attackers. A successful attack not only jeopardises customer confidence in the FI's internal control systems and processes but also causes real financial loss when trade secrets and proprietary information are divulged. FIs should identify important data and adopt adequate measures to detect and prevent unauthorised access, copying or transmission of confidential information.

9.1.2 The FI should develop a comprehensive data loss prevention strategy to protect sensitive or confidential information, taking into consideration the following specifications:

a. Data at endpoint - Data which resides in notebooks, personal computers, portable storage devices and mobile devices;

b. Data in motion - Data that traverses a network or that is transported between sites; and

[8] Cyber attacks include phishing, denial of service attacks, spamming, sniffing, spoofing, hacking, key-logging, phishing, middleman interception, and other malware attacks from mutating virus and worms.

c. Data at rest - Data in computer storage which includes files stored on servers, databases, backup media and storage platforms.

9.1.3 To achieve security of data at endpoints, the FI should implement appropriate measures to address risks of data theft, data loss and data leakage from endpoint devices, customer service locations and call centres. The FI should protect confidential information stored in all types of endpoint devices with strong encryption.

9.1.4 The FI should not use unsafe internet services such as social media sites, cloud-based internet storage sites, and web-based emails to communicate or store confidential information. The FI should implement measures to prevent and detect the use of such services within the FI.

9.1.5 For the purpose of exchanging confidential information between the FI and its external parties, the FI should take utmost care to preserve the confidentiality of all confidential information. For this purpose, the FI should at all times take appropriate measures including sending information through encrypted channels (e.g. via encrypted mail protocol) or encrypting the email and the contents using strong encryption with adequate key length. The FI should send the encryption key via a separate transmission channel to the intended recipients. Alternatively, the FI may choose other secure means to exchange confidential information with its intended recipients.

9.1.6 Confidential information stored on IT systems, servers and databases should be encrypted and protected through strong access controls, bearing in mind the principle of "least privilege"[9].

9.1.7 The FI should assess various methods in which data could be securely removed from the storage media and implement measures to prevent the loss of confidential information through the disposal of IT systems. In determining the appropriate media sanitisation method to use, the FI should take into consideration security requirements of the data residing on the media.

9.2 Technology Refresh Management

9.2.1 To facilitate the tracking of IT resources, the FI should maintain an up-to-date inventory of software and hardware components used in the production and disaster recovery environments which includes all relevant associated

[9] Least privilege is defined as assigned privileges on a "need-to-have" basis.

warranty and other support contracts related to the software and hardware components.

9.2.2 The FI should actively manage its IT systems and software so that outdated and unsupported systems which significantly increase its exposure to security risks are replaced on a timely basis. The FI should pay close attention to the product's end-of-support ("EOS") date as it is common for vendors to cease the provision of patches, including those relating to security vulnerabilities that are uncovered after the product's EOS date.

9.2.3 The FI should establish a technology refresh plan to ensure that systems and software are replaced in a timely manner. The FI should conduct a risk assessment for systems approaching EOS dates to assess the risks of continued usage and establish effective risk mitigation controls where necessary.

9.3 Networks and Security Configuration Management

9.3.1 The FI should configure IT systems and devices with security settings that are consistent with the expected level of protection. The FI should establish baseline standards to facilitate consistent application of security configurations to operating systems, databases, network devices and enterprise mobile devices within the IT environment.

9.3.2 The FI should conduct regular enforcement checks to ensure that the baseline standards are applied uniformly and non-compliances are detected and raised for investigation. The FI should ensure that the frequency of enforcement reviews is commensurate with the risk level of systems.

9.3.3 The FI should deploy anti-virus software to servers, if applicable, and workstations. The FI should regularly update anti-virus definition files and schedule automatic anti-virus scanning on servers and workstations on a regular basis.

9.3.4 The FI should install network security devices, such as firewalls as well as intrusion detection and prevention systems, at critical junctures of its IT infrastructure to protect the network perimeters. The FI should deploy firewalls, or other similar measures, within internal networks to minimise the impact of security exposures originating from third party or overseas systems, as well as from the internal trusted network. The FI should on a regular basis, also back

up and review rules on network security devices to determine that such rules are appropriate and relevant.

9.3.5 FIs deploying Wireless Local Area Networks (WLAN) within the organisation should be aware of risks associated in this environment. Measures, such as secure communication protocols for transmissions between access points and wireless clients, should be implemented to secure the corporate network from unauthorised access.

9.4 Vulnerability Assessment and Penetration Testing

9.4.1 Vulnerability assessment (VA) is the process of identifying, assessing and discovering security vulnerabilities in a system. The FI should conduct VAs regularly to detect security vulnerabilities in the IT environment.

9.4.2 The FI should deploy a combination of automated tools and manual techniques to perform a comprehensive VA. For web-based external facing systems, the scope of VA should include common web vulnerabilities such as SQL injection and cross-site scripting.

9.4.3 The FI should establish a process to remedy issues identified in VAs and perform subsequent validation of the remediation to validate that gaps are fully addressed.

9.4.4 The FI should carry out penetration tests in order to conduct an in-depth evaluation of the security posture of the system through simulations of actual attacks on the system. The FI should conduct penetration tests on internet-facing systems at least annually.

9.5 Patch Management

9.5.1 The FI should establish and ensure that the patch management procedures include the identification, categorisation and prioritisation of security patches. To implement security patches in a timely manner, the FI should establish the implementation timeframe for each category of security patches.

9.5.2 The application of patches, if not carried out appropriately, could potentially impact other peripheral systems. As such, the FI should perform rigorous testing of security patches before deployment into the production environment.

9.6 Security Monitoring

9.6.1 Security monitoring is an important function within the IT environment to detect malicious attacks on IT systems. To facilitate prompt detection of unauthorised or malicious activities by internal and external parties, the FI should establish appropriate security monitoring systems and processes.

9.6.2 The FI should implement network surveillance and security monitoring procedures with the use of network security devices, such as intrusion detection and prevention systems, to protect the FI against network intrusion attacks as well as provide alerts when an intrusion occurs.

9.6.3 The FI should implement security monitoring tools which enable the detection of changes to critical IT resources such as databases, system or data files and programs, to facilitate the identification of unauthorised changes.

9.6.4 The FI should perform real-time monitoring of security events for critical systems and applications, to facilitate the prompt detection of malicious activities on these systems and applications.

9.6.5 The FI should regularly review security logs of systems, applications and network devices for anomalies.

9.6.6 The FI should adequately protect and retain system logs to facilitate any future investigation. When determining the log retention period, the FI should take into account statutory requirements for document retention and protection.

10 DATA CENTRES PROTECTION AND CONTROLS

10.0.1 As FIs' critical systems and data are concentrated and maintained in the DC, it is important that the DC is resilient and physically secured from internal and external threats.

10.1 Threat and Vulnerability Risk Assessment

10.1.1 The purpose of a Threat and Vulnerability Risk Assessment ("TVRA") is to identify security threats to and operational weaknesses in a DC in order to determine the level and type of protection that should be established to safeguard it.

10.1.2 The assessment of threats and vulnerabilities relating to a DC will vary depending on a number of factors, such as criticality of the DC, geographical location, multi-tenancy and type of tenants occupying the DC, impact from natural disasters, and the political and economic climate of the country in which the DC resides. The FI should base its TVRA assessment on various possible scenarios of threats which include theft, explosives, arson, unauthorised entry, external attacks and insider sabotage.

10.1.3 The FI should include in the scope of the TVRA a review of the DC's perimeter and surrounding environment, as well as the building and DC facility. The FI should also review daily security procedures, critical mechanical and engineering systems, building and structural elements as well as physical, operational and logical access controls.

10.1.4 When selecting a DC provider, the FI should obtain and assess the TVRA report on the DC facility. The FI should verify that TVRA reports are current and that the DC provider is committed to address all material vulnerabilities identified. For the FI that chooses to build its own DC, an assessment of threats and vulnerabilities should be performed at the feasibility study stage.

10.2 Physical Security

10.2.1 The FI should limit access to DC to authorised staff only. The FI should only grant access to the DC on a need to have basis. Physical access of staff to the DC should be revoked immediately if it is no longer required.

10.2.2 For non-DC personnel such as vendors, system administrators or engineers, who may require temporary access to the DC to perform maintenance or

repair work, the FI should ensure that there is proper notification of and approval for such personnel for such visits. The FI should ensure that visitors are accompanied at all times by an authorised employee while in the DC.

10.2.3 The FI should ensure that the perimeter of the DC, DC building, facility, and equipment room are physically secured and monitored. The FI should employ physical, human and procedural controls such as the use of security guards, card access systems, mantraps and bollards where appropriate.

10.2.4 The FI should deploy security systems and surveillance tools, where appropriate, to monitor and record activities that take place within the DC. The FI should establish physical security measures to prevent unauthorised access to systems, equipment racks and tapes.

10.3 Data Centre Resiliency

10.3.1 To achieve DC resiliency, the FI should assess the redundancy and fault tolerance in areas such as electrical power, air conditioning, fire suppression and data communications.

10.3.2 The FI should rigorously control and regulate the environment within a DC. Monitoring of environmental conditions, such as temperature and humidity, within a DC is critical in ensuring uptime and system reliability. The FI should promptly escalate any abnormality detected to management and resolve the abnormality in a timely manner.

10.3.3 The FI should implement appropriate fire protection and suppression systems in the DC to control a full scale fire if it occurs. The FI should install smoke detectors and hand-held fire extinguishers in the DC and implement passive fire protection elements, such as fire walls around the DC, to restrict the spread of a fire to a portion of the facility.

10.3.4 To ensure there is sufficient backup power, the FI should install backup power consisting uninterruptible power supplies, battery arrays, and/or diesel generators.

11 ACCESS CONTROL

11.0.1 Three of the most basic internal security principles[10] for protecting systems are:

a. Never alone principle - Certain systems functions and procedures are of such sensitive and critical nature that FIs should ensure that they are carried out by more than one person at the same time or performed by one person and checked by another. These functions may include critical systems initialisation and configuration, PIN generation, creation of cryptographic keys and the use of administrative accounts.

b. Segregation of duties principle - Segregation of duties is an essential element of internal controls. The FI should ensure that responsibilities and duties for operating systems function, systems design and development, application maintenance programming, access control administration, data security, librarian and backup data file custody are separated and performed by different groups of employees. It is also desirable that job rotation and cross training for security administration functions be instituted. The FI should design the transaction processes so that no single person may initiate, approve, execute and enter transactions into a system for the purpose of perpetuating fraud or in a manner that would conceal the transaction details.

c. Access control principle – The FI should only grant access rights and system privileges based on job responsibility and the necessity to have them to fulfil one's duties. The FI should check that no person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities. The FI should only allow staff with proper authorisation to access confidential information and use system resources solely for legitimate purposes.

11.1 User Access Management

11.1.1 The FI should only grant user access to IT systems and networks on a need-to-use basis and within the period when the access is required. The FI should ensure that the resource owner duly authorises and approves all requests to access IT resources.

[10] These internal control principles can be adapted depending on separation of responsibilities, division of duties, environmental variables, systems configurations and compensating controls, where relevant, physical security is imputed in applicable control principles and practices.

11.1.2 Employees of vendors or service providers, who are given authorised access to the FI's critical systems and other computer resources, pose similar risks as the FI's internal staff. The FI should subject these external employees to close supervision, monitoring and access restrictions similar to those expected of its own staff.

11.1.3 For accountability and identification of unauthorised access, the FI should ensure that records of user access are uniquely identified and logged for audit and review purposes.

11.1.4 The FI should perform regular reviews of user access privileges to verify that privileges are granted appropriately and according to the 'least privilege' principle. The process may facilitate the identification of dormant and redundant accounts as well as detection of wrongly provisioned access.

11.1.5 Passwords represent the first line of defence, and if not implemented appropriately, they can be the weakest link in the organisation. Thus, the FI should enforce strong password controls over users' access to applications and systems. Password controls should include a change of password upon first logon, minimum password length and history, password complexity as well as maximum validity period.

11.1.6 The FI should ensure that no one has concurrent access to both production systems and backup systems, particularly data files and computer facilities. The FI should also ensure that any person who needs to access backup files or system recovery resources is duly authorised for a specific reason and a specified time only. The FI should only grant access for a specific purpose and for a defined period.

11.2 Privileged Access Management

11.2.1 Information security ultimately relies on trusting a small group of skilled staff, who should be subject to proper checks and balances. Their duties and access to systems resources should be placed under close scrutiny. The FI should apply stringent selection criteria and thorough screening when appointing staff to critical operations and security functions.

11.2.2 Some common tactics used by insiders to disrupt operations include planting logic bombs, installing stealth scripts and creating system backdoors to gain unauthorised access as well as sniffing and cracking passwords. System

administrators[11], IT security officers, programmers and staff performing critical operations invariably possess the capability to inflict severe damage on critical systems they maintain or operate by virtue of their job functions and privileged access.

11.2.3 The FI should closely supervise staff with elevated system access entitlements and have all their systems activities logged and reviewed as they have the knowledge and resources to circumvent systems controls and security procedures. The FI should adopt the following controls and security practices:

a. Implement strong authentication mechanisms such as two-factor authentication for privileged users;

b. Institute strong controls over remote access by privileged users;

c. Restrict the number of privileged users;

d. Grant privileged access on a "need-to-have" basis;

e. Maintain audit logging of system activities performed by privileged users;

f. Disallow privileged users from accessing systems logs in which their activities are being captured;

g. Review privileged users' activities on a timely basis;

h. Prohibit sharing of privileged accounts;

i. Disallow vendors and contractors from gaining privileged access to systems without close supervision and monitoring; and

j. Protect backup data from unauthorised access.

[11] For the purpose of this document, "system administrators" refer to persons who are granted privileged access to maintain or operate systems, computer equipment, network devices, security tools, databases and applications.

12 ONLINE FINANCIAL SERVICES[12]

12.0.1 Whilst the internet presents opportunities for FIs to reach new markets and expand its range of products and services, being an open network, it also brings about security risks that are more sophisticated and dynamic than closed networks and proprietary delivery channels. The FI should be cognisant of risks that are brought about as a result of the FI offering its financial services via the internet platform.

12.0.2 There are varying degrees of risks associated with different types of services provided over the internet. Typically, financial services offered via the internet can be classified into information service[13], interactive information exchange service[14] and transactional service[15]. The highest level of risk is associated with transactional service as online transactions are often irrevocable once executed.

12.0.3 FIs should clearly identify risks associated with the types of services being offered in the risk management process. The FI should also formulate security controls, system availability and recovery capabilities, which commensurate with the level of risk exposure, for all internet operations.

12.1 Online Systems Security

12.1.1 More attacks may be targeted at FIs' internet systems as financial services are increasingly being provided via the internet and more customers transact on this platform. As a counter-measure, the FI should devise a security strategy and put in place measures to ensure the confidentiality, integrity and availability of its data and systems.

[12] Online financial services refer to the provision of banking, trading, insurance or other financial services and products via electronic delivery channels based on computer networks or internet technologies, including fixed line, cellular or wireless networks, web-based applications and mobile devices.

[13] Information service is the most basic form of online internet service. It is a one-way communication whereby information, advertisements or promotional material are provided to the customers.

[14] Interactive information exchange service allows customers to communicate with the FI, make account enquiries and fill in application forms to take up additional services or purchase new products offered.

[15] Transactional service allows customers to execute online transactions such as the transfer of funds, payment of bills and other financial transactions.

12.1.2 The FI should provide its customers and users of its internet services the assurance that online login access and transactions performed over the internet on the FI's website are adequately protected and authenticated.

12.1.3 MAS expects an FI to properly evaluate security requirements associated with its internet systems and adopt encryption algorithms which are of well-established international standards and subjected to rigorous scrutiny by an international community of cryptographers or approved by authoritative professional bodies, or government agencies (Refer to Appendix C on Cryptography for details).

12.1.4 The FI should ensure that information processed, stored or transmitted between the FI and its customers is accurate, reliable and complete. With internet connection to internal networks, financial systems and devices may now be potentially accessed by anyone from anywhere at any time. The FI should implement physical and logical access security to allow only authorised staff to access its systems. The FI should also implement appropriate processing and transmission controls to protect the integrity of systems and data.

12.1.5 The FI should implement monitoring or surveillance systems so that it is alerted to any abnormal system activities[16], transmission errors or unusual online transactions. The FI should establish a follow-up process to verify that these issues or errors are adequately addressed subsequently.

12.1.6 The FI should maintain high resiliency and availability of online systems and supporting systems (such as interface systems, backend host systems and network equipment). The FI should put in place measures to plan and track capacity utilisation as well as guard against online attacks. These online attacks may include denial-of-service attacks (DoS attack) and distributed denial-of-service attack (DDoS attack) (Refer to Appendix D for details).

12.1.7 FIs should implement two-factor authentication[17] at login for all types of online financial systems and transaction-signing for authorising transactions. The primary objectives of two-factor authentication and transaction-signing are to secure the customer authentication process and to protect the integrity of

[16] An example of the abnormal system activities includes multiple sessions using an identical customer account originating from different geographical locations within a short time span.

[17] Two-factor authentication for system login can be based on any two of the factors, i.e. What you know (e.g. PIN), What you have (e.g. OTP token) and Who you are (e.g. Biometrics).

customer account data and transaction details as well as to enhance confidence in online systems by combating cyber attacks targeted at FIs and their customers.

12.1.8 For FIs which provide online financial systems servicing institutional investors, accredited investors or corporate entities, where alternate controls and processes are implemented to authorise transactions, the FI should perform a risk assessment on such systems to ensure that the level of security for these controls and processes, are equivalent or better than using token-based mechanisms to authorise transactions.

12.1.9 The FI should also take appropriate measures to minimise exposure to other forms of cyber attacks such as middleman attack which is more commonly known as a man-in-the-middle attack[18] (MITMA), man-in-the browser attack or man-in-the application attack (Refer to Appendix E for details).

12.1.10 As more customers log onto FIs' websites to access their accounts and conduct a wide range of financial transactions for personal and business purposes, the FI should put in place measures to protect customers who use online systems. In addition, the FI should educate its customers on security measures that are put in place by the FI to protect the customers in an online environment. The FI should ensure that its customers have access to continual education to raise the security awareness of customers (Refer to Appendix F for details on Customer Protection and Education).

12.2 Mobile Online Services and Payments Security

12.2.1 Mobile Online Services refers to the provision of financial services via mobile devices such as mobile phones or tablets. Customers may choose to access these financial services via web browsers on mobile phones or the FI's self-developed applications on mobile platforms such as Apple's iOS, Google's Android and Microsoft's Windows operating systems.

12.2.2 Mobile payment refers to the use of mobile devices to make payments. These payments may be made using various technologies such as near-field communication (NFC).

[18] In a man-in-the-middle attack, an interloper is able to read, insert and modify messages between two communicating parties without either one knowing that the link between them has been compromised. Possible attack points for MITMA could be customer computers, internal networks, information service providers, web servers or anywhere in the internet along the path between the customer and the FI's server.

12.2.3 Mobile online services and payments are extensions of the online financial services and payments services which are offered by FIs and accessible from the internet via computers or laptops. The FI should implement security measures which are similar to those of online financial and payment systems on the mobile online services and payment systems. The FI should conduct a risk assessment to identify possible fraud scenarios and put in place appropriate measures to counteract payment card fraud via mobile devices.

12.2.4 As mobile devices are susceptible to theft and loss, the FI should ensure that there is adequate protection of sensitive or confidential information used for mobile online services and payments. The FI should have sensitive or confidential information encrypted to ensure the confidentiality and integrity of these information in storage and transmission. The FI should perform the processing of sensitive or confidential information in a secure environment.

12.2.5 The FI should educate its customers on security measures to protect their own mobile devices from viruses and other errant software which cause malicious damage and have harmful consequences.

13 PAYMENT CARD SECURITY (AUTOMATED TELLER MACHINES, CREDIT AND DEBIT CARDS)

13.0.1 Payment cards[19] allow cardholders the flexibility to make purchases wherever they are. Cardholders may choose to make purchases by physically presenting these cards for payments at the merchant or they could choose to purchase their items over the internet, through mail-order or over the telephone. Payment cards also provide cardholders with the convenience of withdrawing cash at automated teller machines ("ATMs") or merchants.

13.0.2 Payment cards exist in many forms; with magnetic stripe cards posing the highest security risks. Sensitive payment card data stored on magnetic stripe cards is vulnerable to card skimming attacks. Card skimming attacks can happen at various points of the payment card processing, including ATMs, payment kiosks[20] and EFTPOS terminals.

13.0.3 Types of payment card fraud include counterfeit, lost/stolen, card-not-received[21] ("CNR") and card-not-present[22] ("CNP") fraud.

13.1 Payment Card Fraud

13.1.1 An FI which provides payment card services should implement adequate safeguards to protect sensitive payment card data. The FI should ensure that sensitive payment card data is encrypted to ensure the confidentiality and integrity of these data in storage and transmission, and the processing of sensitive or confidential information is done in a secure environment.

13.1.2 The FI should deploy secure chips to store sensitive payment card data. The FI should also implement strong card authentication methods such as dynamic data authentication ("DDA") or combined data authentication ("CDA") methods for online and offline card transactions. As magnetic stripe cards are vulnerable to card skimming attacks, the FI should ensure that magnetic stripes are not used as a means to store sensitive or confidential information

[19] For the purpose of this document, "payment cards" refer to ATM, credit, charge and debit cards.

[20] For the purpose of this document, "payment kiosks" refer to merchant provided 24-hour payment kiosks such as self-service automated machines (SAM) and AXS machines.

[21] Card-not-received fraud refers to fraud cases where cardholders do not receive cards dispatched by the issuing banks and subsequently, these cards are used to make fraudulent transactions.

[22] Card-not-present fraud involves the use of stolen or compromised card details to make purchases over the internet, phone or mail order.

for payment cards. For interoperability reasons, where transactions could only be effected by using information from the magnetic stripe on a card, the FI should ensure that adequate controls are implemented to manage these transactions.

13.1.3 For transactions that customers perform with their ATM cards, the FI should only allow online transaction authorisation. The FI card issuer, and not a third party payment processing service provider, should perform the authentication of customers' sensitive static information, such as PINs or passwords. The FI should perform regular security reviews of the infrastructure and processes being used by its service providers.

13.1.4 The FI should ensure that security controls are implemented at payment card systems and networks.

13.1.5 The FI should only activate new payment cards sent to a customer via post upon obtaining the customer's instruction.

13.1.6 The FI should implement a dynamic one-time-password ("OTP") for CNP transactions via internet to reduce fraud risk associated with CNP.

13.1.7 To enhance card payment security, the FI should promptly notify cardholders via transaction alerts when withdrawals / charges exceeding customer-defined thresholds made on the customers' payment cards. The FI should include in the transaction alert, information such as the source and amount of the transaction.

13.1.8 The FI should implement robust fraud detection systems with behavioural scoring or equivalent; and correlation capabilities to identify and curb fraudulent activities. The FI should set out risk management parameters according to risks posed by cardholders, the nature of transactions or other risk factors to enhance fraud detection capabilities.

13.1.9 The FI should follow up on transactions exhibiting behaviour which deviates significantly from a cardholder's usual card usage patterns. The FI should investigate these transactions and obtain the cardholder's authorisation prior to completing the transaction.

13.2 ATMs and Payment Kiosks Security

13.2.1 The presence of ATMs and payment kiosks (e.g. SAM and AXS machines) has provided cardholders with the convenience of withdrawing cash as well as making payments to billing organisations. However, these systems are targets where card skimming attacks are perpetrated.

13.2.2 To secure consumer confidence in using these systems, the FI should consider putting in place the following measures to counteract fraudsters' attacks on ATMs and payment kiosks:

a. Install anti-skimming solutions on these machines and kiosks to detect the presence of foreign devices placed over or near a card entry slot;

b. Install detection mechanisms and send alerts to appropriate staff at the FI for follow-up response and action;

c. Implement tamper-resistant keypads to ensure that customers' PINs are encrypted during transmission;

d. Implement appropriate measures to prevent shoulder surfing of customers' PINs; and

e. Conduct video surveillance of activities at these machines and kiosks; and maintain the quality of CCTV footage.

13.2.3 The FI should verify that adequate physical security measures are implemented at third party payment kiosks, which accept and process the FI's payment cards.

14 IT AUDIT

14.0.1 As technology risks evolve with the growing complexity of the IT environment, there is an increasing need for FIs to develop effective internal control systems to manage technology risks.

14.0.2 IT audit provides the board of directors and senior management with an independent and objective assessment of the effectiveness of controls that are applied within the IT environment to manage technology risks.

14.0.3 The FI should establish an organisational structure and reporting lines for IT audit in a way that preserves the independence and objectivity of the IT audit function.

14.1 Audit Planning and Remediation Tracking

14.1.1 The FI should ensure that the scope of IT audit is comprehensive and includes all critical IT operations.

14.1.2 An IT audit plan, comprising auditable IT areas for the coming year, should be developed. The IT audit plan should be approved by the FI's Audit Committee.

14.1.3 The FI should establish an audit cycle that determines the frequency of IT audits. The audit frequency should be commensurate with the criticality and risk of the IT system or process.

14.1.4 Consequently, a follow-up process to track and monitor IT audit issues, as well as an escalation process to notify the relevant IT and business management of key IT audit issues, should be established.

APPENDIX A: SYSTEMS SECURITY TESTING AND SOURCE CODE REVIEW

A.1 Overview

A.1.1 The FI should conduct rigorous testing of systems to verify the security, reliability and availability of its systems under normal and extreme conditions. However, security testing by itself is ineffective in identifying or detecting security threats and weaknesses such as malicious codes, trojans, backdoors, logic bombs and other malware. Thus, the FI should include in its system development life cycle (SDLC) a review of the system source code to identify and detect such threats and weaknesses in its systems.

A.1.2 The FI should take note of the following areas during system testing and source code review:

a. Information Leakage

The FI should ensure that sensitive or confidential information such as cryptographic keys, account details, passwords, system configurations and database connection strings are protected. Hence, the FI should scrutinise potential sources of information leakages like verbose error messages and banners, hard-coded data, files and directories operations for accidental information disclosure.

b. Resiliency Against Input Manipulation

One common security weakness in applications is the failure to properly validate inputs, from a user or system interface. Malformed inputs can spawn major vulnerabilities such as script injection and buffer overflows as well as cause erratic system behaviour. The FI should ensure that data validation includes the following steps:

i. all inputs to an application should be validated;

ii. all forms of data (such as text boxes, select boxes and hidden fields) should be checked;

iii. the handling of null and incorrect data input should be verified;

iv. content formatting should be checked; and

v. maximum length for each input field should be validated.

All input validation routines should be reviewed and tested to assess their effectiveness against known vulnerabilities.

c. Unsafe Programming Practices

The FI should ensure that the source code review enables it to identify unsafe programming practices such as the use of vulnerable function calls, poor memory management, unchecked argument passing, inadequate logging and comments, use of relative paths, logging of passwords and authentication credentials, as well as assignment of inappropriate access privilege.

d. Deviation From Design Specifications

Implementation oversight is one of the common causes of system vulnerabilities. The FI should review critical modules such as those containing authentication and session management functions for any deviation from its design specifications. Testing of authentication functions should cover the verification of security requirements (such as credential expiry, revocation and reuse) and the protection of cryptographic keys. The FI should test session management to ensure that:

i. sensitive or confidential information that is stored in cookies is encrypted;

ii. the session identifier is random and unique; and

iii. the session expires after a pre-defined length of time.

e. Cryptographic Functions

The strength of cryptography depends not only on the algorithm and key size, but also on its implementation. The FI should evaluate cryptographic implementation and ensure that only cryptographic modules based on authoritative standards and reputable protocols are installed. The FI should review cryptographic algorithms and crypto-key configurations for deficiencies and loopholes. The choice of ciphers, key sizes, key exchange control protocols, hashing functions and random number generators should be thoroughly assessed. Rigorous testing should be conducted on all cryptographic operations (encryption, decryption, hashing, signing) and key management procedures (generation, distribution, installation, renewal, revocation and expiry) (Refer to Appendix C for more details).

f. Exception Handling

When exception or abnormal conditions occur, the FI should ensure that adequate controls are in place so that resulting errors do not allow users to bypass security checks or obtain core dumps. The FI should also ensure that sufficient processing details are logged at the source of the exception to assist problem diagnosis. Robust exception/error handling that facilitates fail-safe processing under various exception conditions should be implemented. Leakage of sensitive or confidential information due to improper error handling should be prevented.

g. Business Logic

The FI should test its business logic to ensure that a user cannot perform an unauthorised function or transaction. It is imperative that negative testing be included in the testing to determine the response of a system when an unexpected input is received.

h. Authorisation

After a user has been authenticated and gains access into the system, authorisation helps to ensure that the user is only allowed to view, write, execute, modify, create and/or delete data and invoke the functions that he is permitted to do so. FI should perform tests to confirm that the actual access rights granted to a user in the system conform to the approved security access matrix.

i. Logging

Logging is implemented to facilitate follow-up investigation and troubleshooting when a system incident occurs. The FI should build the following requirements and specifications into the tests:

i. sensitive or confidential information such as passwords, authentication credentials, cryptographic keys, confidential business data should not be recorded in system logs;

ii. the maximum data length for logging is pre-determined;

iii. successful and unsuccessful authentication attempts are logged; and

iv. successful and unsuccessful authorisation events are logged.

APPENDIX B: STORAGE SYSTEM RESILIENCY

B.1 Overview

B.1.1 Storage systems are key IT infrastructure components that house critical data. The resiliency and availability of these storage systems are crucial to the continuous operation of critical applications and online systems used by FIs.

B.2 Reliability and Resiliency

B.2.1 The FI should regularly review the architecture and connectivity of storage systems used by critical applications for single points of failure and fragility in functional design and specifications, as well as technical support, whether performed in-house or by vendors. The FI should also consider the resiliency of storage systems for both centralised and distributed systems.

B.2.2 Where SANs are deployed, the FI should incorporate redundancy in all SAN components. A poorly designed SAN presents concentration risk to the FI's system infrastructure. The FI should install multiple links and switches for all Input/Output operations between hosts, adapters, storage processors and storage arrays. Due to the criticality of SAN, a high availability, resilient and flexible SAN architecture should be established.

B.2.3 To improve the reliability and fault-tolerant capability of storage systems, the FI should establish a sound patch management process to update its storage systems with the latest stable and proven microcode release on a timely basis. The FI should ensure that the deployment of configuration changes and upgrades to storage systems is governed by a rigorous change management process.

B.2.4 The FI should establish an in-house alert and monitoring capability for early detection of warnings and outages in its storage systems, as well as data replication mechanisms. The FI should consider the implementation of vendor call-home capability to perform advanced diagnostics and remediation. To minimise the risk of multiple failures, human errors and security breaches, the FI should maintain oversight of diagnostics and remediation activities, whether performed in-house or by vendors.

B.3 Recoverability

B.3.1 In the event of a major site outage, the FI should ensure that the architecture of the storage system has the capability to switch over from the primary production site to an alternate site to meet expected RTO and RPO. The FI should regularly test the recoverability and consistency of data at the alternate site.

APPENDIX C: CRYPTOGRAPHY

C.1 Principles of Cryptography

C.1.1 The primary application of cryptography is to protect the integrity and privacy of sensitive or confidential information. Cryptography is also commonly used in FIs to protect sensitive customer information such as PINs relating to critical applications (e.g. ATMs, payment cards and online financial systems).

C.1.2 All encryption algorithms used in a cryptographic solution should depend only on the secrecy of the key and not on the secrecy of the algorithm. As such, the most important aspect of data encryption is the protection and secrecy of cryptographic keys used, whether they are master keys, key encrypting keys or data encrypting keys.

C.2 Cryptographic Algorithm and Protocol

C.2.1 Constant advances in computer hardware, computational number theory, cryptanalysis and distributed brute force techniques may induce larger key lengths to be used in future. Some contemporary cipher algorithms may also have to be enhanced or replaced when they lose their potency in the face of ever increasing computer speed and power.

C.2.2 The FI should vet functions involving cryptographic algorithms and crypto-key configurations for deficiencies and loopholes. While conducting this review, the FI should also evaluate the choice of ciphers, key sizes, key exchange control protocols, hashing functions and random number generators.

C.2.3 Random Number Generators are used in many algorithms and schemes as a construct component. The security of many cryptographic algorithms depends upon the unpredictable quality of a random seed. The FI should ensure that there is sufficient size and randomness of the seed number to preclude the possibility of optimised brute force attack.

C.3 Cryptographic Key Management

C.3.1 Cryptographic key management policy and procedures covering generation, distribution, installation, renewal, revocation and expiry should be established.

C.3.2 The FI should ensure that cryptographic keys are securely generated. The FI should destroy all materials used in the generation process after usage, and

ensure that no single individual knows any key in its entirety or has access to all the constituents making up these keys. The FI should ensure that all keys are created, stored, distributed or changed under stringent conditions.

C.3.3 The FI should ensure that unencrypted symmetric keys are entered into the tamper-resistant device, such as hardware security module, only in the form of at least two components using the principles of dual control. Cryptographic keys should be used for a single purpose to reduce the impact of an exposure of a key.

C.3.4 The effective timeframe that a cryptographic key may be used in a given cryptographic solution is called the cryptoperiod. The FI should consider and decide the appropriate cryptoperiod for each cryptographic key. The sensitivity of data and operational criticality should determine the frequency of key changes.

C.3.5 The FI should ensure that hardware security modules and keying materials are physically and logically protected.

C.3.6 When cryptographic keys are being used or transmitted, the FI should ensure that these keys are not exposed during usage and transmission.

C.3.7 When cryptographic keys have expired, the FI should use a secure key destruction method to ensure keys could not be recovered by any parties.

C.3.8 In the event of changing a cryptographic key, the FI should generate the new key independently from the previous key.

C.3.9 The FI should maintain a backup of cryptographic keys. The same level of protection as the original cryptographic keys should be accorded to backup keys.

C.3.10 If a key is compromised, the FI should immediately revoke, destroy and replace the key and all keys encrypted under or derived from the exposed key. The FI should inform all parties concerned of the revocation of the compromised keys.

APPENDIX D: DISTRIBUTED DENIAL-OF-SERVICE PROTECTION

D.1 Overview

D.1.1 Although DDoS attacks have always posed a formidable threat to internet systems, the proliferation of botnets and the advent of new attack vectors together with the rapid adoption of broadband globally in recent years have fuelled the potency of such attacks.

D.1.2 In addition, the evolving threat landscape for internet systems has resulted in more sophisticated DDoS attacks focusing on other layers (e.g. layer 7) of the Open System Interconnection model, which could be accomplished with minimal bandwidth.

D.1.3 The normal amount of network bandwidth and system capacity sizing of even a large commercial organisation is unlikely to withstand a sustained DDoS offensive by a sizeable botnet or a group of botnets. The immense quantity of computing resources amassed by botnets to unleash an attack would rapidly deplete the network bandwidth and processing resources of a targeted system, inevitably inflicting massive service disruption or cessation.

D.1.4 Notwithstanding that most FIs have instituted effective safeguards to protect its systems from malware such as trojans and worms, which may cause them to become unwitting members of botnets, more should be done to bolster system robustness against DDoS attacks.

D.2 Detecting and Responding to DDoS Attacks

D.2.1 An FI providing online financial services should be responsive to unusual network traffic conditions, volatile system performance or a sudden surge in system resource utilisation as these may be symptomatic of a DDoS onslaught. The FI should deploy appropriate anti-DDoS equipment to facilitate the detection of and response to DDoS attacks. The success of any pre-emptive and reactive actions hinges on the deployment of appropriate tools to effectively detect, monitor and analyse anomalies in networks and systems.

D.2.2 As part of the defence strategy, the FI should install and configure adequate devices such as application and network firewalls, network and host-based intrusion detection/preventions systems, routers and other specialised equipment to alert security staff and divert and/or filter network traffic in real-time once an attack is suspected or confirmed. As DDoS attacks may result in a significant volume of traffic, the FI should consider the use of purpose-built

appliances designed for high-speed performance. The objective here is to remove malicious packets so that legitimate traffic en route to the internet banking and trading systems could flow through.

D.2.3 Potential bottlenecks and single points of failure vulnerable to DDoS attacks could be identified through source code review, network design analysis and configuration testing. The elimination of these weaknesses would improve system resilience.

D.3 Selection of Internet Service Providers

D.3.1 Without the co-operation of internet service providers (ISPs), many organisations find the task of foiling DDoS attacks daunting. An effective countermeasure would often rely on the ISPs to dampen an attack in upstream networks.

D.3.2 Given that a collaborative approach should be adopted by FIs and its ISPs, it is important that the FI incorporates DDoS attack considerations in its ISP selection process where the FI should determine:

a. whether an ISP offers DDoS protection or clean pipe services to assist in detecting and deflecting malicious traffic;

b. the ability of the ISP to scale up network bandwidth on demand;

c. the adequacy of an ISP's incident response plan; and

d. the ISP's capability and readiness in responding quickly to an attack.

D.4 Incident Response Planning

D.4.1 The FI should devise an incident response framework and routinely validate the framework to facilitate fast response to a DDoS onslaught or an imminent attack. The FI should include in this framework a plan detailing the immediate steps to be taken to counter an attack, invoke escalation procedures, activate service continuity arrangements, trigger customer alerts, and report any such attack to MAS.

D.4.2 The FI should be familiar with its ISPs' incident response plans and assimilate them into its incident response framework. To foster better co-ordination, the FI should establish a communication protocol between the FI and its ISPs and conduct periodic joint incident response exercises.

APPENDIX E: SECURITY MEASURES FOR ONLINE SYSTEMS

E.1 Overview

E.1.1 A MITMA refers to a scenario where an interloper is able to read, insert and modify at will, messages between two communicating parties without either one knowing that the link between them has been compromised.

E.1.2 There are many possible attack points for MITMA. They may be at customer computing devices, internal networks, information service providers, web servers or anywhere along the path between the user and an FI's server.

E.2 Security Measures

E.2.1 As part of the two-factor authentication infrastructure, the FI should implement adequate controls and security measures to minimise exposure to man-in-the middle attacks.

E.2.2 In respect of transaction signing for high-risk transactions[23], which include high value transactions, the FI should

a. use digital signatures and key-based message authentication codes (KMAC) to detect unauthorised modification or injection of transaction data in a MITMA;

b. ensure that the customer using a hardware token is able to distinguish the process of generating a one-time password from the process of digitally signing a transaction and what he signs digitally is meaningful to him[24]; and

c. use different crypto keys for generating OTPs and for signing transactions.

E.2.3 The FI may choose to implement challenge-based or time-based OTPs for its online systems. OTPs provide strong security because their period of validity is controlled entirely by FIs and does not depend on the user's behaviour.

[23] High-risk transactions would include changes to sensitive customer data (e.g. customer office and home address, email and telephone contact details), registration of third party payee details and revision of funds transfer limits.

[24] For example, for transfer of funds, the information to be signed should be meaningful i.e. payee account number, the payment amount, etc.

Time-based OTPs require a time window to be configured at the server side. The FI should establish a time window that is as short as practicable to lower the risks of OTP misuse.

E.2.4 Customers should be notified, through a second channel, of high-risk transactions as well as payment or fund transfer above a specified value determined by customers. The notifications should contain meaningful information such as type of transaction and payment amounts. The FI should send the notification to the customer's device that is not used to perform the transaction.

E.2.5 Besides Secure Socket Layer (SSL), the FI should implement end-to-end encryption security at the application layer so that customer PINs and passwords are not exposed at any intermediate nodes between the browser and the host where PINs and passwords are verified.

E.2.6 An online session should be automatically terminated after a fixed period of time unless the customer is re-authenticated. This prevents an attacker from keeping an internet session alive indefinitely.

E.2.7 The FI should ensure that its customers using the internet application are informed about how they should react to SSL server certificate warning. Customers should terminate a login session if a SSL certificate does not belong to the FI and a warning is given to this effect. As part of customer security awareness program, the FI should advise its customers to inform the FI immediately of such warning messages.

APPENDIX F: CUSTOMER PROTECTION AND EDUCATION

F.1 Overview

F.1.1 Direct attacks on online financial systems have caused customer PINs to become increasingly vulnerable. Through targeted attacks, customer PINs are under constant threats from various types of systems vulnerabilities, security flaws, exploits and scams. The FI should ensure that customers' accounts and data are protected and raise customers' security awareness with regard to using online financial services.

F.2 Customer Protection

F.2.1 FIs should not distribute software to its customers via the internet or through a web-based system unless they can provide adequate security and safeguards for the customers. This is to avoid situations whereby customers are deceived by hackers into downloading trojans, backdoors, viruses and other malware which cause damage and harmful consequences to them. Appropriate measures should be implemented to alert and assist customers in verifying the origin and integrity of the downloaded software.

F.2.2 The following control measures should be observed when handling customers' login credentials for online applications:

a. Implement dual control and/or segregation of duties in the generation of passwords, printing of password mailers and activation of online accounts;

b. Print password mailers in a secure location where physical access is restricted and monitored;

c. Destroy all mailer spoilages immediately and generate a new password for each reprint;

d. Destroy all stationery which may contain any password imprint during mailer printing;

e. Strengthen password dissemination process to ensure that passwords are not being exposed or compromised;

f. Ensure that passwords are not processed, transmitted or stored in clear-text;

g. Require customers and system users to change issued passwords immediately upon first login; and

h. Only distribute a hardware token that has been assigned to a customer account.

F.2.3 Customers should be informed about the risks and benefits of using online financial services before they subscribe to such services. The FI should inform customers clearly and precisely of the respective rights, obligations and responsibilities of the customers and the FI on all matters relating to online transactions, and in particular, any problems that may arise from processing errors and security breaches. The FI should present the information in an easy to understand format.

F.2.4 The FI should make the terms and conditions applying to online financial services readily available to customers within the internet application. On initial logon or subscription to a particular service, the FI should require a positive acknowledgement of the terms and conditions from the customer.

F.2.5 The FI should also post these other forms of disclosures on its website.

a. Customer privacy and security policy.

b. Customer dispute handling, reporting and resolution procedures, including the expected timing for the FI's response. The FI should set out on its website an explanation on the process to resolve the problem or dispute, as well as the conditions and circumstances in which the resultant losses or damages would be attributable to the FI or its customers if security breaches occur.

c. Security measures and reasonable precautions customers should take when accessing their online accounts. The precautionary procedures would include taking adequate steps to prevent unauthorised transactions and fraudulent use of their accounts, as well as making sure that no one else would be able to observe or steal their access credentials or other security information to impersonate them or obtain unauthorised access to their online accounts.

F.2.6 The FI should ensure that an authenticated session, together with its encryption protocol, remains intact throughout the interaction with the customer. In the event of interference, the FI should put in place measures to ensure that the session is terminated and the affected transactions are

resolved or reversed out. The FI should promptly notify the customer of such an incident as the session is being concluded or subsequently by email, telephone or through other means.

F.3 Customer Education

F.3.1 The FI should educate its customers on the security and reliability of their interaction with FIs. Customer's confidence in the safety and soundness of the FI's online products and services depends to a large extent on their understanding of and compliance with the security requirements related to the operation of their online accounts and transaction services. In addition, it is important that customers understand the need to take appropriate security measures to protect their devices and computer systems.

F.3.2 When new operating features or functions for the online financial services, the FI should ensure that sufficient instruction and information on the new features and functions are provided to its customers. Continual education and timely information provided to customers will help them to understand the security requirements and take appropriate steps in reporting security problems.

F.3.3 To raise security awareness, the FI should remind its customers on the need to protect their PINs, security tokens, personal details and other confidential data. The FI should ensure that static PIN and OTP security instructions are displayed prominently in the user login page or the USER ID, PIN and OTP entry page. The following guidelines would be useful in helping customers to construct robust PINs and adopt better security procedures:

a. PIN should be at least 6 digits or 6 alphanumeric characters.

b. PIN should not be based on guessable information such as user-id, personal telephone number, birthday or other personal information.

c. PIN should be kept confidential and not be divulged to anyone.

d. PIN should be memorised and not be recorded anywhere.

e. PIN should be changed regularly or when there is any suspicion that it has been compromised or impaired.

f. The same PIN should not be used for different websites, applications or services, particularly when they relate to different entities.

g. Customer should not select the browser option for storing or retaining user name and password.

h. Customer should check the authenticity of the FI's website by comparing the URL and the FI's name in its digital certificate or by observing the indicators provided by an extended validation certificate.

i. Customer should check that the FI's website address changes from 'http://' to 'https://' and a security icon that looks like a lock or key appears when authentication and encryption is expected.

j. Customer should not allow anyone to use or tamper with his OTP security token.

k. Customer should not reveal the OTP generated by his security token to anyone.

l. Customer should not divulge the serial number of his security token to anyone.

m. Customer should check his account information, balance and transactions frequently and report any discrepancy.

n. Customer should inform the FI immediately on the loss of his mobile phones or change in his mobile phone numbers.

F.3.4 The FI should advise its customers to adopt the following security precautions and practices:

a. Install anti-virus, anti-spyware and firewall software in their personal computers and mobile devices.

b. Update operating systems, anti-virus and firewall products with security patches or newer versions on a regular basis.

c. Remove file and printer sharing in computers, especially when they are connected to internet.

d. Make regular backup of critical data.

e. Consider the use of encryption technology to protect highly sensitive or confidential information.

f. Log off the online session.

g. Clear browser cache after the online session.

h. Do not install software or run programs of unknown origin.

i. Delete junk or chain emails.

j. Do not open email attachments from strangers.

k. Do not disclose personal, financial or credit card information to little-known or suspect websites.

l. Do not use a computer or a device which cannot be trusted.

m. Do not use public or internet café computers to access online services or perform financial transactions.

F.3.5 In view of the widespread use of payment cards such as ATM, credit and debit cards, customers should be educated on the features of these cards as well as the associated risks. The FI should provide adequate information and instructions its customers on the security features of their cards and the steps to report card loss or fraud cases.

F.3.6 The above information on security precautions and good practices is not intended to be exhaustive nor static. The FI should provide updated security information and best practice guidelines to customers in a user-friendly manner.